P.4 1 type copy to H.C.S.G.
Sigs. 6. W.O.
P.4 Please
Enquire DDY. WO.
27/9.

15(I)

TOP SECRET

TICOM/I-113

# INTERROGATION OF MAJOR DR. RUDOLF HENTZE

## HEAD OF GRUPPE IV (CRYPTANALYSIS).

## GENERAL DER NACHRICHTENAUF-

### KLAERUNG

The attached is a composite report based on the preliminary interrogation by Major FLINT, AUS, at ICKING on 14th June 1945 and subsequent interrogations at REVIN by Major BUNDY, AUS, and Capts. LAWRANCE AND CAMPBELL I.C. between 11th and 15th July, 1945. Attached as appendices are:- (a) a chart of the organisation of Gen d NA in general and of Gruppe IV in particular, and (b) a short report on the solution of M 209, both prepared by HENTZE. P/W has since been released.

TICOM

No. of pages: 12

18th September, 1945

DISTRIBUTION

British

D.D.3
H.C.G.
D.D.(N.S.)
D.D.(M.W.)
D.D.(A.S.)
C.C.R. (2)
Lt. Col. Leathem
Cdr. Tandy
Major Morgan

TICOM

Chairman
S.A.C.(2)
Cdr.Bacon
Lt.Col. Johnson
Major Seaman
Lt. Cdr. Manson
Capt. Cowan
Lt. Fehl
Ticom Files (4)

U.S.

Op-20-G (2) (via Lt.Cdr. Manson)
G-2 (via Lt. Col. Hilles)
A.S.A. (3) (via Major Seaman)
Director, S.I.D. USFET
(via Lt.Col. Johnson)
Col. Lewis Powell, USSTAF

ADDITIONAL

S.A.C. for Signals 6, W.O.
S.A.C. for .D.D.Y., W.O.

I. Personal History

Major HENTZE was born and has lived most of his life in the KASSEL area of Germany. In 1933 he received his Doctor of Philosophys' degree from MARBURG University. His specialities have been mathematics, statistics and philosophy. He taught and was student adviser in various schools in the KASSEL area. He was a lieutenant in the Engineer Corps of the German Army during the first World War. Between the two wars P/W remained a member of the Reserve Officers'Corps.

In 1935, while writing a book on Mathematics and Statistics P/W develcped a keen interest in cryptanalysis. During the period from 1935 until the outbreak of hostilities he was keenly interested in the mathematical relationship of the letter frequencies in various encipherment methods. At the outbreak of the war in 1939 P/W came to active duty as a captain in charge of an engineer supply depot in the BAD KREUZNACH area. In 1940 his wife died and he received a transfer to his home area so that he could take care of his two children. He was transferred to KASSEL and worked as personnel Adjutant in a replacement headquarters in the KASSEL area.

In 1942 the German High Command called for methematical experts to be used in Cryptanalysis. P/W was called upon and sent for training to BERLIN. After a several month course, he was transferred to Kommandeur 5 at ST GERMAIN, near PARIS, in June, 1942. He remained there in charge of the Cryptanalytical Section until the Germans were forced to withdraw from that area. In November 1944 P/W was transferred to a position in charge of the cryptanalytical section of General der Nachrichten Aufklaerung. He remained in this position until the end of hostilities.

P/W is a benevolent-looking man of at least 55. His attitude under interrogation was completely co-operative, and he did not seem to be holding back anything. The impression of interrogators is that his mind is far from brilliant and definitely slow-moving. He could not answer many questions at once, but if given a day to think it over would come up with something. His membry for names is particularly faulty. He seemed childishly proud of the success achieved in his work in the West, and his inability to describe the work of sections under him in Gen der NA seemed to bear out the mediocre opinion of his abilities previously expressed by KARRENBERG and others.

II Movements of KDR. 5

On leaving LOUVECIENNES about mid-August 1944 they went first to VIGGINGEN (?) near METZ, and moved again at the beginning of September to KROPDORF near GIESSEN. Form there in March they went to the RHOEN and finally to DISCHINGEN in the DONAUWOERTH area.

III Cipers

(a) M.209: This was broken only on depths. His estimate of the traffic per month intercepted was 1,000 messages; in this they would find about 50 cases of depth, and break a total of about 30% of the

/intercepts

intercepts. P/W does not remember specific units with which special success was achieved. (At a later interrogation he showed that he knew the M.209

(See also Appendix B).

(b)Strip: This was a system using 25 strips, with indicators URSAL USABU. The contents were mixed military and diplomatic. It was solved in 1942 and 1943 until succeded by M.209. The strips for a period would be recovered by In 7/VI, and Kdr. 5 would work only with known strips. P/W remembers broken traffic from USA to England and North Africa both. 70% - 80% of the traffic could be read, and about 50 groups were required for a break-in. In 1944 a new system appeared using 30 strips, which could not be broken.

(c)Slidex: This was extensively read, MP nets in particular being a fertile source of intelligence. British and Americans were equally bad in their use of it, particularly in employing Slidex for messages which should have gone in a more secure system. They were able to break currently and in many cases five or six hours after the start of the day. One of the main aids to entry was the fact that operators used the left-hand alphabet almost exclusively. They were able to break in before the invasion and could hold on, with the help of cribs and stereotyped language, in spite of the improvement in operators' habits after September. Asked for specific cases of insecure units, P/W quoted the "2nd Airborne Division", 'CCA' and 'CCB' (Note: this looks like a confusion. These are terms used in American Armoured divisions: the 2nd was in the Northern sector of the American front during the campaign). P/W commented that they were much happier with a message wholly in slidex than with a mixed clear and cipher message, which did not give so many frequencies.

This is a copy
The original has
been retained under
section 3(4) of the
Public Records Act
1958.

/(d)

(d) W.O.C.: All P/W had to say was that it had ben read up to the time Kom. 621 was captured in North Africa in July 1942, but not thereafter.

(e) An American 25 x 25 table (possibly 26 x 26) formed by a keyword plus the rest of the alphabet, this being written backwards and upwards, same keyword top and side: daily changing. P/W said this was used by a single division in the latter part of 1944, after they moved to KROFDORF, in the Southern area Wouth of MAINZ. The table was systematic, with mixed code and letter values. A stereotyped message at 0400 hours, each day reporting 'No change' enabled them to read most of this traffic.

(f) Maplay: This was worked on throughout 1944. The volume of traffic was low and they found it harder to solve than Slidex. They were successful only if they had a lot of traffic or a re-encodement from Slidex. (This latter had provided the original break). They found Unicode easier than Maplay.

(g) Prearranged 3-letter codes: They had considerable success with these. At first they were only changed every month. Later it was every eight days, but even so they were solved by the 4th or 5th day.

(h) MATIN: This was never solved. Statistically they arrived at the conclusion that it was a small machine but had no real idea what it was. P/W did not say clearly whether this was worked on at Kdr. 5 or, as seems more likely, at OKH.

(i) '999': This was 5-digit traffic, with ten tables, used for practice only in the pre-invasion period. The tables were reconstructed, but it was never operational.

(j) Machine ciphers: Typex had been studied, but without success. P/W felt they would have got somewhere if they had ever got hold of a model of it or of the American 'big machine'; but they had no luck.

On Enigma, P/W said they had learned from a Polish officer that the Poles had read it before stecker was introduced, and that stecker had been brought in in consequence.

The French C36 had been solved analytically; it was easier than M.209. 624 Komp. at MONTPELLIER and 625 had had practical success with it.

The Croat enigma (i.e. their Allies, not Tito or Mihailovic) was being solved up to the end of the war.

/(k)

(k) Double Transposition: The Germans had been successful on this as used by the Croats and Tito. KUHNEL (of ref 5, Gen der NA) had said the English usage was theoretically soluble, but they had never done it in practice. (P/W seemed very woolly on this, was not even sure whether it was an Army system or not).

IV Organisation of Gen D NA (See Appendix B)

ANDRAE:- former head of LNA. Intercept and not crypto. Seen at the end of April, not thereafter by P/W.

MARQUARDT:- had been Kdr. 5, took over Gruppe I in November 1944. Function of this Gruppe was to advise on the dispositon of KONAs in the field. M. had very few personnel in the Gruppe and did not do much.

THIEL:- had been with LNA for a long time, and was thoroughly familiar with the West problem. Had about 50 people in the Gruppe and produced radio sitreps correlating the information from Kdrs. 5, 6 and 7. Decodes of traffic regularly broken were handled at KONA level and evaluated there, copies going back to Gruppe II for later use in its reports. P/W remarked there that Gruppe IV did no operational breaking at any time on the Western traffic.

GORZOLLA:- also former LNA man. His section co-ordinated Eastern D/F results with decodes. Much of the latter was NKWD which was broken in Gruppe IV and passed to Gruppe III.

BLOCK:- P/W knew nothing about Gruppe V or BLOCK.

GRUPPE VI:- ROEDER did Russian work himself, while the American work was done by Insp. HELLER. The Gruppe was located in Potsdam. The American traffic intercepted was "Weltverkehr", thought byP/W to be machine traffic. He said that Gruppe IV had begun work on it, and sent an Uffz. (P/W didn't know name) to Gruppe VI to bring back traffic. They had had no success with it, however. Gruppe IV also sent a man (again P/W could'nt recall the name: it must have been KARRENBERG) to see about the Russian. P/W knew only of 5 figure traffic in the BAUDOT, and said that efforts had been made to use the chat("Verstaendnisverkehr"). All this work was just beginning in November 1944 when P/W came to Gruppe IV (confirms KARRENBERG), and the intercept apparatus he said, was in POTSDAM. H. did not know whether the apparatus was pinched from the Russians or built up from scratch.

GRUPPE IV:- Referat 1 was the research Ref. MARQUARDT he described as a mathematician who used to be with In 7/VI. He also spoke of Wachtmeister HILBURG as a mathematician in the Ref. H. said this Referat worked on Slidex, Codex, "999" and M.209 steadily and not simply as a research proposition. (His previous statement that it was not done operationally probably still holds good. Unless communications were very good, they must have simply kept their hand in and tackled especially interesting or difficult days, or traffic that looked as if it had tricks in it).

H. said this Ref. also worked on Russian 4 and 5 figure enciphered codes and had partial success working from depths.

/He

He was unable to give details on this.

Ref. 1A:- Uffz. CHRISTMANN was given as another member of this.

Ref. 1B:- Wachtmeister DOERING was mentioned. Said to be specialist in M.209. Also said to have worked on "big machine" without success. Sdf. LUZIUS was also said to be very good and specialist in M.209.

Ref. 2A:- Uffz KEHR's name was given. Work of section said to be English hand systems, as Slidex, Codex, etc., in regular way. (Sounds like duplication of effort, but we could get no more on the work of this section).

Ref. 2B:- Sdf. KUEHN (different from Obinsp. KUEHN) and Obgefr. VUHRISCH, also a Wachtmeister of whom P/W could remember nothing except that he had a French wife and the Gestapo had once got on to him for a letter he had written in French. Section worked on French hand systems.

Ref. 2C:- Wm. ESTERHAZY mentioned. This man about 30 years old and worked on Hungarian, Croat, Serbian, also Sdf. GEISSLER on hand systems of same countries.

3A:- Sdf. PESCHKE (BLESCHKE ?) described as Russian speaker, not methematician, worked on enciphered 5 figure Russian code. P/W does not know details of this effort or its success. Wm. SCHMIDT also worked on this, and there were about 20 people in the section.

3B:- Obwm. (? SAMSONOW: P/W could not remember name) was deputy to DETTMANN. Also Uffz. ANDREJEVSKI. About 20 men in section. Had good success, expecially on NIVA code, which did not change for a period of two years and therefore could be read almost entirely up to the end of 1944. This was a 5 figure code enciphered. From it the main lines could be established. A new NIVA came in at the end of 1944 and about 500 groups of this had been recovered by the end of the war. Again, P/W could not give details on methods.

3C:- P/W knew nothing. There were only ten men left when he took over (the Russians not being in Russia any more, he explained, cut down the partisan traffic).

Ref.4:- H. said this section was purely mechanical and had no cryptenalytic personnel. Most of its personnel were women. It was located in a factory in JUTERBOG, in two big rooms on the ground floor and two above. Most of its work was on statistics, some on the sorting and collating of enemy callsigns. Most of the work came from Ref. 1, a little from 2 and 3, such as original work on a anew French code. The section was moved to ERFURT when JUTERBOG was threatened, and set up in a building near the railway station. H. thought one waggon of equipment had gone to BAMBERG. He said the equipment had 30 key punches and two tabulators used to find repeats. He did not know about the details of the rest of the machines. So far as he knew there were no special devices. Section 4C was simply an advanced party sent to Weimar to prepare the way for the rest when they went to ERFURT temporarily to move to W. permanently. However, there had not been enough room and the second move had never been made.

/Ref 5

Ref. 5:- This was the training section that dated all the way back. KUEHN was still in charge, but the students had dwindled to a batch of 40 each three months, in two courses of 20. Most of these came from the Nachrichten-Dolmetscher-Schule. All crypto men for the Army still went through here, and indeed H. himself had studied in the beginning under KUEHN. Uffz. KUHNEL was said to be the best instructor left at the end, a mathematician.

An attempt was made to get more detail. But P/W seemed unable to give particulars on many points. He did not seem to be holding back and came right out with important things. Our impression is that he was simply an amiable supervisor who had neither time, ability, nor inclination to find out all about the section under him. His own field was closest to Refs 1A and 1B and on these he was relatively satisfactory. He admitted he knew very little about Eastern front work.

V. Kdrs 5 and 6

Giving more detail on Kdr 5, P/W gave the following names from his deciphering section:-

Oblt. SCHLEMMER (had been there since 1942)
Wm. ENGELHARDT (mathematician)
Wm. RATHGEBER (Ex-chemist)
Uffzs. FLICK, THUNER and DATO.

P/W said the section had a fair proportion of mathematicians. Most of the men were about 30 years old.

Kdr. 6 was commanded by Major LEICHNER, formerly of In 7/VI. Ltn. V. DENFFER was the chief cryptanalyst, with a staff of about 30. Kdr. 6 was not started until Nov.1944. It exchanged results with Kdr. 5 at first directly, then via KOPP, and finally directly again. They had good success with Slidex on their own, much less with M.209 as they were less experienced and had less traffic.

VI. General

P/W said he had no connection with traffic analysis or DF. His only connection with intercept control was that he would ask for the particular nets that he was able to read. His Entzifferung group did work very closely with the Auswertestelle in the identification of units by c/s, frequency, etc. (In this connection he mentioned particularly the 29th Div., as having very tell-tale habits). On most units it was not too difficult to keep continuity from day to day, without knowing callsign systems at all.

In a digression on D/F in general P/W said that in the West D/F had not been useful after the invasion. Before that it had given a good picture. We asked specifically whether he knew how accurate this picture had turned out to be and he did not know. (He seemed to have no consciousness of any W/T deception on our part, and on all questions of value of intelligence he was very vague and said he only heard at second hand anyway after he passed his decodes on).

/Speaking

Speaking of pre-invasion days. H. said they had a picture of the British units in England before invasion, but not of American ones. They had no information from decodes at this time. He said they did not know the exact date of invasion, but did know the general time and area. They had expected a second push at CALAIS and 613 Komp. had in fact been sent to LILLE especially for this purpose. He remarked in passing here that the intercept companies had done extremely well for them throughout, including the time after they got back to Germany.

P/W said the whole of Gen der NA was last together at REICHENHALL. BOETZEL then broke up the Gruppen and divided the men among the various Kdre. DETTMAN, KUHN and about ten others stayed with BOETZEL, who took to the Alps. He had not seen any of this group since they broke up.

Asked about liaison with Luftwaffe, he said that Kdr 5 worked closely with a Luftwaffe unit located near St.GEMAIN. He does not remember the officers, but says a Feldwebel was in charge of the Entzifferung section af about 10 men. These men were trained by him and became expert at breaking 209 and Slidex, with the results going to the Auswertestelle. Later the Luftwaffe went back to LIMBURG and from SEPTEMBER there was little liaison.

He knew VOEGELE and had seen him once or twice at ST. GERMAIN. He never went to the OKL central place and saw no results from them in his Gen der NA days.

P/W said they had no liaison that he knew of with the Auswaertiges Amt, Navy or Forschungsamt.

He said the HAGUE FHS was under Kdr 5, he visited it once in 42, knew nothing about it beyond regular radio intercept.

TOP SECRET

TICOM/I-113

# APPENDIX A

## GENERAL OF SIGNALS RECCE

Oberst BÖTZEL

Officer z.b.V.

Oberstleutnant ANDRAE

| Gruppe Z | Gruppe I | Gruppe II | Gruppe III | Gruppe IV | Gruppe V | Gruppe VI |
|---|---|---|---|---|---|---|
| Maj.Hüther | Maj.Marquardt. | Hptm.Dr. Thiel. | Hptm. Gorzolla | Maj.Dr. Hentze | Amtmann Block | Hptm. Roeder |
| Staff matters | Tactical control of operations by O.C.s Sigs.Recce. | Compilation of Sigint information (Western area). | Compilation of Sigint information (Eastern area) | Cryptanalysis | Equipment of O.C.s Sigs.Recce | American and Russian Baudot traffic |

## ORGANIZATION AND TASKS OF GRUPPE IV OF GENERAL OF SIGNALS RECCE ((GENERAL DER NACHRICHTEN-AUFKLÄRUNG))

Head of the Gruppe: Major Dr. HENTZE:

Control and Organization of cryptanalysis on army cyphers.

Main Section 1: Regierungs-Baurat Dr. PIETSCH:

Development of new methods of analysis.

Section 1a: Regierungs-Baurat Dr. MARQUARDT:

Examination of unknown hand cyphers.

Section 1b: Regierungs-Baurat Dr. PIETSCH:

Examination of machine cyphers.

Main Section 2: Oberleutnant Dr. KNESCHKE:

Cryptanalysis of cyphers of the western and southern powers.

Section 2a: Regierungs-Baurat Dr. SCHULZ:

Cryptanalysis of British and U.S. cyphers.

Section 2b: Oberinspektor KÜHN:

Cryptanalysis of French cyphers.

Section 2c: Oberleutnant Dr. KNESCHKE:

Cryptanalysis of Balkan, Italian and Spanish cyphers.

Main Section 3: Leutnant DETTMANN:

Cryptanalysis of Russian cyphers.

Section 3a: Inspektor TORUNSKI:

Cryptanalysis of Russian army cyphers.

Section 3b: Leutnant DETTMANN:

Cryptanalysis of N.K.V.D. cyphers.

Section 3c: Wachtmeister FUCHS

Cryptanalysis of partisan cyphers.

Main Section 4: Regierungs-Baurat SCHENKE:

Preliminary cryptanalytical work with Hollerith machines.

Section 4a: Regierungs-Baurat SCHENKE:

Operation of Hollerith machines.

Section 4b: Inspektor SCHÜSSLER :

Repairs workshop.

Section 4c: Wachtmeister WEISS:

Emergency quarters WEIMAR.

Main Section 5: Oberinspektor KÜHN:

Preliminary and further training of cryptanalysts.

Main Section 6: Oberleutnant KOLBE:

In charge of subordinate staff.

---

APPENDIX B.

This is a copy
The original has
been retained under
section 3(4) of the
Public Records Act
1958.

This is a copy
The original has
been retained under
section 3(4) of the
Public Records Act
1958.